Business & Contracting – Module 6

ELO 6.1 **Identify the Cloud-related guidance when contracting for cloud services**

ELO 6.2 **Identify contract and legal considerations related to cloud services acquisition**

ELO 6.3 ***Identify risks of not having a direct contractual relationship with the cloud service provider. (no content on this ELO—maybe not necessary)***

ELO 6.4 ***Identify metrics associated with DoD cloud reporting requirements. (no content on this ELO—maybe not necessary)***

ELO 6.3 **Match key business and contracting terms from the section to appropriate definitions.**

Module – 6: Business & Contracting

Topics

- Overview
- Business Case Analysis
- Cloud Computing Service Acquisition
- Access to Government Data
- Contract Compliance with Cloud Computing SRG
- Cyber Incident Reporting
- Damage Assessment
- Location of Data
- Personnel Requirements
- Service Level Agreement
- Spillage
- Subcontracting
- Match key business and contracting terms from the section to appropriate definitions.

You should be able to:

- Identify the key content that needs to be provided in the Business Case Analysis
- Match cloud-related policy with the guidance provided by the policy.
- Identify contract considerations related to cloud services acquisition, and an associated justification for each consideration.
- Identify risks of not having a direct contractual relationship with the cloud service provider.
- Match key business and contracting terms from the section to appropriate definitions.

Business & Contracting Overview

Topic

Business & Contracting Overview

You should be able to:

Questions

Guidance/Provider	Commercial Cloud	Non-Federal Information System - Cloud	Cloud Federal Information System - Contractor	Cloud Federal Information System – Government
DFARS	X		X	
CCPG	X		X	
DoD CIO Memo	X		X	
SRG	X		X	X
DODI 8500.01			X	X
DODI 8510.01			X	X
NIST SP 800-171		X		

Content

- To address the cloud business and contracting risks identified in Module 4 this module will provide a high level overview of federal regulations and best practices guidance
- The adoption of cloud within the Department represents a dramatic shift in the way the DOD buys IT – a shift from periodic capital expenditures to lower cost and predictable operating expenditures.
- Similar to other IT technology investments, DOD organizations are responsible for acquiring the cloud services that meet their mission objectives and provide an optimal solution compliant with DOD and other federal regulations. The following are important cloud related guidance when contracting for cloud services:
  - Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013–D018). August 26, 2015
  - DISA Cloud Connection Process Guide (CCPG), Version 1.0. July 2015
  - DoD CIO Memorandum: “Updated Guidance on the Acquisition and Uses of Commercial Cloud Computing,” December 15, 2014
  - DoD Cloud Computing Security Requirements Guide (SRG)
  - DoD Instruction 8500.01, Cybersecurity, March 14, 2014
  - DoD Instruction 8510.01, Risk Management Framework for DoD Information Technology, March 12, 2014
  - NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, June 2015
- To determine the appropriate guidance one needs to determine whether a federal information system will be providing the service or a non-federal information system. The definition of a federal information system from NIST SP 800-171: “a federal information system is a system that is used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. An information system that does not meet such criteria is a nonfederal information system.”

Business Case Analysis

Topic

Business Case Analysis

You should be able to:

1. What is the purpose of an IT BCA?
2. Who approves the BCA and who receives a copy
3. The purpose of the BCA
4. Major parts to the BCA

Questions

Content

- The Cloud Computing BCA is required by DOD CIO Memo, "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services", Dec 15, 2014
- Use of cloud services must be analyzed using the IT Business Case Analysis (BCA) template
- DISA provided cloud services must be considered as an alternative in the BCA.
- Component CIO reviews/approves
- Component submits copy of BCA to DoD CIO
- Purpose of the BCA
  - Ensures consistent approach in IT investment analysis
  - Facilitate comparison of alternatives
  - Clearly define expected costs, benefits, operational impacts, and risk
  - Not a requirements validation process
- Major components of BCA
  - Cost and economic viability
  - Requirement satisfaction/completeness
  - Operational benefit (qualitative)
  - Risk Assessment
  - Conclusions and recommendations
    - Balance cost effectiveness with operational benefit
    - Funding type and sources
- The BCA Template is available on the DoD CIO Portal: https://dodcioext.osd.mil (I can't find it after going to this site and searching for it)
- Actually performing a BCA is beyond the scope of this Continuous Learning Module, suffice it so say that the BCA recommends a cloud solution

Cloud Computing Service Acquisition

Topic

Cloud Computing Service Acquisition

You should be able to:

1. Identify the key contracting and legal considerations

Questions

Content

- Once the business case has been made to acquire cloud services, the Component selects a CSP
- Key Cloud-Computing Contracting and Legal Considerations
  - Access to Government data for auditing, FOIA, forensic analysis, inspection, and litigation
  - Cloud Computing SRG Compliance
  - Cyber Incident Reporting
  - Damage Assessment
  - Location of Data
  - Personnel Requirements
  - Service Level Agreements
  - Spillage
  - Subcontracting
- The Component should not use a Government Purchase Card (GPC) to acquire cloud-computing services
  - GPCs are not allowed for reoccurring services
  - GPCs have spending maximums that will likely be exceeded in acquisition of cloud services
  - Accepting the CSP's terms of service (TOS) without modification are likely to result in Anti-deficiency Act (ADA) violation
  - TOS that are deemed acceptable by the Components legal council should be incorporated into the contract with the CSP

Access to Government Data

Topic

Access to Government Data

You should be able to:

Questions

Content

- The Component should ensure the following terms are incorporated into the contract with the CSP to ensure the government has needed access to its data
  - Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.
  - The Contractor shall provide the government, or its authorized representatives, access to all government data and government-related data, contractor personnel involved in performance of the contract, and physical access to any Contractor facility with government data, for the purpose of audits, investigations, inspections, or other similar activities, as authorized by law or regulation.
  - When the Government is using a Contractor's software, the Contractor shall provide the agency with access and the ability to search, retrieve, and produce Government data in a standard commercial format.

Contract Compliance with Cloud Computing SRG

Topic

Contract Compliance with Cloud Computing SRG

You should be able to:

Questions

Content

- The Component needs to ensure the contract with the CSP provides appropriate security for government data
- In accordance with the DOD CIO Memo, "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services", Dec 15, 2014, **public** DoD information can be hosted on FedRAMP approved CSOs after obtaining a DoD PA and the appropriate AO's approval (determined by Mission Owner).
- For more sensitive DoD unclassified data, Components need to follow the DoD Cloud Computing Security Requirements Guide (SRG)
- The Contracting Officer shall ensure that the Contractor implements and maintains the administrative, technical, and physical safeguards and controls within the security level and services specified in the SRG (version in effect at the time the solicitation is issued) found at http://iase.disa.mil/cloud_security/Pages/index.aspx

Cyber Incident Reporting

Topic

Cyber Incident Reporting

You should be able to:

Questions

Content

- The Component needs to ensure the contract with the CSP requires appropriate cyber incident reporting
- When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information therein, conduct a review for evidence of compromise of covered defense information
- When the Contractor discovers a cyber incident the contractor shall rapidly report cyber incidents to DoD at http://dibnet.dod.mil.
- The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software, in accordance with instructions provided by the Contracting Officer.
- Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis or damage assessment.
- When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

Damage Assessment

Topic

Damage Assessment

You should be able to:

Questions

Content

- If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with the forensic analysis requirements of the contract.
- Prior to initiating damage assessment activities, the PCO shall verify that the contract(s) identified in the cyber incident report include(s) DFARS 252.204-7012. If the PCO determines that a contract identified in the report does not contain the clause, the PCO shall notify the requiring activity that damage assessment activities, if required, may be determined to constitute a change to the contract.
- In cases of cyber incidents involving multiple contracts, a single contracting officer will be designated to coordinate with the contractor regarding media submission.
- If the requiring activity requests the contracting officer to obtain media, as defined in DFARS 252.204-7012, from the contractor, the contracting officer shall:
  - Provide a written request for the media
  - Provide the contractor with the Instructions for Media Submission
  - Provide a copy of the request to DC3 (dcise@dc3.mil) and the requiring activity

Location of Data

Topic

Location of Data

You should be able to:

Questions

Content

- The Contractor shall maintain within the United States or outlying areas all Government data that is not physically located on DoD premises, unless the Contractor receives written notification from the Contracting Officer to use another location
- The Contractor shall provide the Government with a list of the physical locations which may contain government data within 20 days with updates on a quarterly basis.
- Some countries require prior permission of the local Data Protection Commissioner before allowing personal information to be transferred out of the country
- More sensitive government data may have further restrictions on the location of data, work with security to define location requirements

Issues associated with storing DoD data in non-US locations

Topic

Storing DoD data in Non-US Locations

You should be able to:

1. Describe the potential location issue with using public cloud services
2. Identify the threats to DoD information hosted on foreign soil
3. Describe the location restrictions for different levels of data

Questions

1. What is the potential location issue with using public cloud services?
2. What are the potential issues with hosting DoD information in a foreign country?
3. True or false can DoD Level 5 data be hosted by a public cloud service provider who could potentially move the data to a foreign location?
4. What is the requirement for hosting DoD Level 6 data?
5. Who can authorize the storing of Level 4 DoD data at a foreign location?

Content

- Customers have limited visibility into where their data is stored
- Customers' data location maybe changed within the Cloud Service Providers' (CSP) infrastructure by the CSP based on a number of different factors including customer usage, data retrieval time requirements, availability requirements, and the costs of storage at different locations
- Many CSP are international organizations
- Different countries have different rules regarding the movement of data into and out of their country and rules regarding the collection of different types of data particularly for Personally Identifiable Information (PII)
- Some countries require prior permission of the local Data Protection Commissioner before allowing personal information to be transferred out of the country
- The US government restricts the transfer of sensitive or classified data to locations outside of the control of US companies or the US government. For example sensitive technology information, information that could potentially impact operational security
- There is the threat that foreign governments could seize sensitive DoD information hosted within their countries either overtly or in a clandestine manner or they could prevent DoD having access to its data
- Level 2 and 4 data is required to be hosted at US, US Territories, or DoD controlled locations unless the location is authorized by the AO
- Level 5 data is required to be hosted at US, US Territories, or DoD controlled locations
- Level 6 data is required to be hosted at locations authorized for classified processing

Cloud Personnel Requirements

Topic

Cloud Personnel Requirements

You should be able to:

Questions

Content

- The Contracting Officer shall ensure any personnel requirements are clearly spelled out for key personnel, minimum proficiency levels/training, proper conduct of staff, and expectations regarding the management of staff.
- The Contactor shall require all employees who will have access to government data, the architecture that supports government data, or any physical or logical devices/code to pass the appropriate background investigation required by the Government in compliance with HSPD -12. At a minimum, all Contractor employees with access to the government data, the architecture that supports government data, or any physical or logical devices/code will pass a National Agency Check and Inquiries (NACI) investigation and be a US person as defined in Executive Order 12333.
- The Contracting Officer shall ensure that the CSP personnel screening and personnel access rules and procedures are appropriate for the information impact level of the CSO and that the CSP is in compliance with the Cloud Computing SRG requirements for the personnel

Service Level Agreement

Topic

Service Level Agreement

You should be able to:

Questions

Content

- Because the government is relinquishing direct control of its data and IT operations, it is important that the Contracting Officer procuring cloud services work with the Mission Owners to develop a Service Level Agreement (SLA) for the contract and incorporate the SLA into the contract with the cloud service provider.
- The SLA should clearly define the contract performance standards, how the contractor will measure performance, and the enforcement mechanisms for SLA compliance.
- The Contract Officer shall also ensure that the contract clearly specifies whether there are any maintenance windows when the CSP expects to affect the cloud service and the CSP notification procedures for planned and unplanned outages.
- The Contract Officer should also clearly define any monitoring and metering requirements the organization has for monitoring the performance of the CSP and capturing the organization's usage patterns and for charging the organization's clients for services.
- The organization should establish process/tools for monitoring the performance and financial costs of the cloud services and alerting the organization when there are significant changes in the performance or cost of cloud services, so that the organization can quickly address changes in

Spillage

Topic

Spillage

You should be able to:

Questions

Content

- The Contractor shall coordinate with the government point of contact provided by the Contracting Officer to respond to any spillage occurring in connection with the cloud services being provided.
- Upon notification by the Government of a spillage, or upon the Contractor's discovery of a spillage, the Contractor shall cooperate with the Contracting Officer to address the spillage in compliance with agency procedures.

Subcontracting

Topic

Subcontracting

You should be able to:

Questions

Content

- When contracting for cloud services the Contracting Officer shall ensure that all terms and conditions flow down to subcontract agreements that the CSP has with its providers of services
- Because of the Privity of Contracts the government has no direct relationship with subcontractors, so it has no ability to enforce the terms of the contract between the prime contractor and the subcontractor
- The prime contractor should also maintain operational configuration control and control of government data (not sure what this has to do with subcontracting).

Business & Contracting Terms

Topic

Business & Contracting Terms

You should be able to:

Match key terms to their definitions

Questions

Match key terms to their definitions

Content

- **Authorizing Official** – as described in DoD Risk Management Framework (RMF) means the senior Federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations organizational assets, individuals, other organizations, and the Nation.
- **Covered Contractor Information System –** means an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.
- **Covered Defense Information –** means unclassified information that is either provided to the contractor by or on behalf of DoD in connection with the performance of the contract or collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract that is controlled technical information, critical information, export control, or other information that is required to be safeguarded by the government.
- **Cyber Incident –** means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. Government data means any information, document, media, or machine readable material regardless of physical form or characteristics, that is created or obtained

Business & Contracting Terms (continued)

Topic

Business & Contracting Terms

You should be able to:

Questions

Content

- **Government-related Data -** means any information, document, media, or machine readable material regardless of physical form or characteristics that is created or obtained by a contractor through the storage, processing, or communication of Government data. This does not include contractor's business records e.g. financial records, legal records etc. or data such as operating procedures, software coding or algorithms that are not uniquely applied to the Government data.
- **Media –** means physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.
- **Privity of Contracts** – contract law that the terms of a contract are only binding on the parties signing the contract
- **Spillage** – security incident that results in the transfer of classified or controlled unclassified information onto an information system not accredited (i.e., authorized) for the appropriate security level.

Recapitulation of Modules – 1, 2, 3, 4, 5, 6

Topic

Review Previous Content

Content

You should be able to:

Questions

Module 7 - Review

Topic

Summary

Content

You should be able to:

Questions

Module 7 – Summary Questions

Topic

Summary

Content

You should be able to:

Questions